

**IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE**

**PATENT APPLICATION
FOR:**

CHARGING MECHANISM FOR MULTICASTING

INVENTOR:

Lin XU, and
Jarno LEINONEN

Morgan & Finnegan, L.L.P.
345 Park Avenue
New York, New York 10154-0053
(212) 758-4800
(202) 857-7887

Attorneys for Applicant

2007780-022002

CHARGING MECHANISM FOR MULTICASTING

CROSS-REFERENCE TO A RELATED APPLICATION

This application for letters patent is related to and incorporates by reference United States patent application serial number TBD titled "A System and Method for Efficient Distribution of Multicastable Services" and filed in the United States Patent and Trademark Office on December 5 6, 2001.

FIELD OF THE INVENTION

The invention disclosed herein is a method, system, and computer program product for calculating a cost of receiving multicast data from a multicast session. In particular, the method, system, and computer program product calculates the cost of receiving multicast data based on either the elapsed time that a user connects to a multicast session, or the volume of data received at a destination during the connection period.

BACKGROUND OF THE INVENTION

A one-to-many or many-to-many Internet Protocol (IP) application involves one or multiple sources sending IP messages to multiple receivers. Exemplary applications include the transmission of corporate messages to employees, communication of stock quotes to brokers, video and audio conferencing for remote meetings and telecommuting, and replicating databases and web site information. The IP multicast protocol efficiently supports one-to-many or many-to-many applications by allowing a source to send a single copy of a message to any recipient who explicitly requests to receive the message. IP multicast is more efficient than a point-to-point unicast protocol that requires the source to send an individual copy of a message to each requester thereby limiting the number of receivers by the bandwidth available to the sender. IP

multicast is also more efficient than a broadcast protocol that sends one copy of a message to every node on the network even though many of the nodes may not want the message and the broadcast protocol is limited to a single subnet. Furthermore, the IP multicast protocol is applicable not only to wired networks, but also wireless networks. For example, in wireless network, link level multicasting allows several terminals to receive data sent over a single air interface.

IP Multicast is a receiver-based protocol. A receiver subscribes to a multicast session group by sending a join message to the multicast session group. Since the network infrastructure delivers the traffic to each member of the multicast session group, the sender does not need to maintain a list of receivers. The advantage is that only one copy of a multicast message passes over any link in the network. In addition, IP Multicast only creates a copy of the message when the paths diverge at a router. Thus, IP multicast yields many performance improvements and conserves bandwidth throughout the system.

IP multicast is an extension to the standard IP network-level protocol. RFC 1112, titled "Host Extensions for IP Multicasting" and authored by Steve Deering in 1989, describes IP multicasting as "the transmission of an IP datagram to a 'host group', a set of zero or more hosts identified by a single IP destination address. IP multicasting delivers a multicast datagram to every member of the destination host group with the same 'best-efforts' reliability as regular unicast IP datagrams. The membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group. A host may be a member of more than one group at a time." In addition, at the application level, a single group address may have multiple data streams on different port

numbers, on different sockets, in one or more applications. Multiple applications may share a single group address on a host.

Multicast communications to establish host membership in a multicast group (e.g., a join message) utilize a standard, such as the Internet Group Management Protocol (IGMP), that supports multicast communication at the Open System Interconnection (OSI) data link layer (layer 2). W. Fenner, Internet Group Management Protocol, Version 2, Request for Comments (RFC) 2236, November, 1997, describe IGMP.

In a shared transport media network, encryption takes place at the Open Systems Initiative (OSI) link level (level 2) to prevent an unintended user on the same point-to-multipoint link to get the multicast packets. Alternatively, Internet Protocol security (IPsec) and tunneling can achieve the same result. In addition, in a shared transport network, it is difficult for a provider to determine a total charge to associate with a multicast service between a source and a user because the total charge comprises a content charge and a delivery charge. The source determines the fee associated with the content charge based on the copyright of the content, the volume of data, or a digital right management (DRM) solution. In contrast, the resources consumed during the delivery of the content to a user such as a content provider dictate the delivery charge. In a wireless network, for example, the resources consumed may include wireless radio resources. The content provider is the owner of the multicast data source, however the actual data may be obtained from a third party who owns the copyright to the content.

The content charge and the delivery charge also differ because the content charge accrues against the user and the delivery charge can accrue against either the content provider or the user. If the delivery charge accrues against the content provider for sending the content over a physical

network, the accrual of the charge can be on a program basis, a data volume basis, or a time basis. Accrual of the delivery charge against the content provider is suitable for delivering content such as an advertisement because the content delivery benefits the content. The disadvantage, however, is that accrual of the delivery charge against the content provider requires a service agreement between the content provider and the network operator. Thus, when the delivery charge accrues against the content provider, it is not possible to charge for delivery of multicast services originating from any content provider on Internet. If the delivery charge accrues against the user for receiving the content over a physical network, it is difficult to track the volume of data that the user receives. Thus, only two types of charging mechanisms are possible, flat rate charging and program or file based charging. Flat rate charging requires the user to periodically pay a fixed price for using the service. Program or file based charging requires the user to pay a fee for each request to receive a program or file. In response to the payment, the user receives an encryption key that will allow access to the program or file. The program or file can include a software application, audio/video file, or graphic image. The encryption scheme can include link level encryption or IPsec.

Sophisticated and cost-effective charging mechanisms, such as time based charging and data volume based charging, have taken the place of flat rate charging and program or file based charging mechanisms. A charging scheme based on connection time will calculate a fee for a service based on the amount of time that a user connects to the service. For example, if a network operator determines that the rate for using a video service is \$5.00 per hour, a user connecting to the video service to view a movie for thirty-minutes accrues a fee of \$2.50. A charging scheme based on the volume of data will calculate a fee for a service based on the volume of data that a user receives from the service. For example, if a network operator

determines that the rate for using a video service is \$0.25 per Megabyte of data received, the fee for a user to use the video service to view a movie consisting of 25 Megabytes is \$6.25.

Currently, time based charging and data volume based charging mechanisms are not available for IP multicast deployed in a network with shared transport media. Since it is difficult to determine when a user has stopped using a shared transport media service, it is difficult for network to calculate the connection time or data volume received. For example, user may establish a multicast connection through a digital broadcast network, but when the battery in the user's terminal loses a charge, the connection is broken without any indication of disjoining the service. Thus, the charging will continue even though the multicast service is no longer in use. Furthermore, security is a problem because the user has the possibility to disjoin the service, but still receives the data from the shared transport media service. This invention disclosed here is one possible solution to establish a secure billing system for multicast service in a network that is capable for link level multicasting.

Thus, there is a need for a system, method, and computer program product for calculating a cost of receiving multicast data from a multicast session. The system, method, and computer program product will calculate the cost of receiving multicast data based on either the elapsed time that a user connects to a multicast session, or the volume of data received at a destination during the connection period. The system, method, and computer program product disclosed herein establish a secure billing system for multicast services in a network that provides link level multicasting.

SUMMARY OF THE INVENTION

A method, system, and computer program product for calculating a cost of receiving multicast data from a multicast session. A multicast network includes at least one multicast

service, each multicast service including at least one multicast session. The method, system, and computer program product receives a request to establish a connection to the multicast session, the request including a start time for the connection and an end time for the connection. The method, system, and computer program product stores the start time for the connection and the end time for the connection and, after termination of the connection, calculates the cost of receiving the multicast data.

The method, system, and computer program product can receive a subsequent request to extend the connection, the subsequent request specifying a new end time for the connection, and store the new end time for the connection. Alternatively, the method, system, and computer program product can receive a subsequent request to terminate the connection, the subsequent request specifying a new end time that precedes the end time for the connection, and store the new end time for the connection.

In one embodiment, the storing of the start time for the connection and the end time for the connection is to a database.

To calculate the cost, the method, system, and computer program product computes a charge for receiving the multicast data, stores the charge, and computes the cost by multiplying the charge by a fee for the multicast service associated with the multicast session. In one embodiment, the storing of the charge is to a database. The method, system, and computer program product can compute an elapsed connection time by subtracting the start time for the connection from the end time for the connection. Alternatively, the method, system, and computer program product can compute a volume of data received over the connection from the start time for the connection to the end time for the connection.

In another embodiment, time is divided into evenly spaced time slots such that the start time for the connection the end time for the connection can only occur at the end of a time slot. Alternatively, the end time for the connection in the request is specified as a discrete number of time slots.

5 In another embodiment, the system for calculating a cost of receiving multicast data from a multicast session includes a collection device and an interface device. The collection device is a general-purpose computer configured to receive a request to establish a connection to the multicast session, the request including a start time for the connection and an end time for the connection, store the start time for the connection and the end time for the connection, and after
10 termination of the connection, calculate the cost of receiving the multicast data. The interface device is a general-purpose computer configured to configure the collection device and display the cost of receiving the multicast data.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying figures best illustrate the details of the system, method, and computer program product that establishes a secure billing system for multicast services in a network that provides link level multicasting, both as to its structure and operation. Like reference numbers
15 and designations in the accompanying figures refer to like elements.

Figure 1A is a network diagram that illustrates an operating environment of a secure billing system for multicast network services in a network that provides link level multicasting.

20 Figure 1B is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1A.

Figure 1C is a network diagram illustrating an embodiment of the secure billing system shown in Figure 1A that accommodates an indirect connection between user terminal 110 and multicast data network 105.

Figure 1D is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1C.

Figure 1E is a network diagram illustrating an embodiment of the secure billing system shown in Figure 1A that distributes the security function to base station 140 and the charging function to charging server 150.

Figure 1F is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1E.

Figure 1G is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1E.

Figures 2A and 2B illustrate a method of operation for the secure billing system shown in Figure 1B.

Figures 2C and 2D illustrate a method of operation for the secure billing system shown in Figure 1G.

Figure 3A is an exemplary timeline for a charging scheme based on connection time that illustrates an explicit disjoin.

Figure 3B is an exemplary timeline for a charging scheme based on connection time that illustrates an implicit disjoin.

Figure 3C is an exemplary timeline for a charging scheme based on slotted connection time that illustrates an explicit disjoin.

Figure 3D is an exemplary timeline for a charging scheme based on slotted connection time that illustrates an implicit disjoin.

Figure 4A is an exemplary timeline for a charging scheme based on data volume that illustrates an explicit disjoin.

Figure 4B is an exemplary timeline for a charging scheme based on data volume that illustrates an implicit disjoin.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1A is a network diagram that illustrates an operating environment of a secure billing system for multicast network services in a network that provides link level multicasting. Internet 100 and multicast data network 105, as shown in Figure 1A, are public communication networks that support multicast delivery of data packets, in general, and multicast delivery of Internet protocol (IP) data packets, in particular. The invention disclosed herein contemplates network architectures comparable to Internet 100 and multicast data network 105 such as a cellular network, a satellite network, a digital video broadcasting (DVB) network, or a private network architecture. Private network architectures include a local area network, a personal area network such as a Bluetooth network, an intranet, or an extranet. An intranet is a private communication network that provides an organization, such as a corporation, with a secure means for trusted members of the organization to access the resources on the organization's network. In contrast, an extranet is a private communication network that provides an organization, such as a corporation, with a secure means for the organization to authorize non-members of the organization to access certain resources on the organization's network. The invention disclosed herein also contemplates network protocols such as Ethernet, Token Ring, and proprietary network protocols comparable to the Internet protocol.

As shown in Figure 1A, user terminal 110 includes an interface module that connects a user to the secure billing system for multicast network services. In one embodiment, user terminal 110 is a general-purpose computer. User terminal 110 also includes a communication module to communicate with devices on multicast data network 105 to receive multicast session data from devices on Internet 100. A user operates user terminal 110 to receive multicast content 195 by sending join request 117 to last hop router 120. After receiving join request 117, last hop router 120 attaches to the multicast tree using any existing multicast routing protocol. In one embodiment, last hop router 120 attaches to the multicast tree via border gateway 180. Last hop router 120 and border gateway 180 perform routing functions for multicast data network 105. Last hop router 120 is the last routing entity that handles data passing from multicast capable data network 105 to user terminal 110. For example, last hop router 120 may be a general-purpose router in a wireless local area network (WLAN) or a Serving General Packet Radio Service (GPRS) Support Node (SGSN) in a GPRS or Universal Mobile Telecommunications System (UMTS) network. Border gateway 180 is the routing entity that provides the interface between multicast data network 105 and an external network such as Internet 100. In response to join request 117, user terminal 110 receives decryption key 118 from multicast data network 105. In one embodiment, last hop router 120 is responsible for sending decryption key 118 to user terminal 110 and encrypts the data sent by multicast server 190 prior to forwarding the data to user terminal 110. In addition to data routing, last hop router 120 monitors multicast communication messages that user terminal 110 sends and receives, stores charging data related to a subscription request, and forwards the charging data to billing server 170, a general-purpose server computer. Billing server 170 converts the charging data into billing data, stores the billing data, and notifies the user of the total charge for subscribing to multicast content 195.

In another embodiment of the secure billing system shown in Figure 1A, multicast data network 105 is a visiting wireless network for user terminal 110. Since billing server 170 is not in the home network for user terminal 110, billing server 170 forwards any billing data for user terminal 110 to the home billing server (not shown) in the home network (not shown) for user terminal 110. The home network (not shown) will connect to either multicast data network 105 or Internet 100 via a connecting border gateway (not shown).

In another embodiment of the secure billing system shown in Figure 1A, the functions comprising collection of the charging data that last hop router 120 performs are distributed throughout multicast data network 105 to reduce the processing load imposed upon last hop router 120. For example, if the charging data includes connection time data and throughput volume data, last hop router 120 can be responsible for collecting the time data and an intermediate router (not shown) along the multicast tree in multicast data network 105 can be responsible for collecting the throughput volume data.

In another embodiment of the secure billing system shown in Figure 1A, the operator of multicast data network 105 provides the multicast service. Thus, multicast server 190 is located in multicast data network 105.

In another embodiment of the secure billing system shown in Figure 1A, billing server 170 is located in another physical network such as Internet 100 and connects with multicast data network 105 via a Virtual Private Network (VPN). Alternatively, last hop router 120 can also include the functionality performed by billing server 170. Thus, last hop router 120 will include a module that converts charging data into billing data, stores the billing data temporarily and periodically forwards the billing data to a billing center.

Figure 1B is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1A. User terminal 110 comprises service discovery 111, multicast session management 112, and multicast security client 113. Service discovery 111 enables the terminal to discover multicast sessions by providing the user with a list of available
5 multicast sessions and the cost associated with each session. Multicast session management 112 is responsible for establishing a multicast session, maintaining the session communication, and disconnecting the session when the communication is complete. Multicast security client 113 manages the security associated with receiving multicast data from a network connection. For example, multicast security client 113 periodically receives decryption key 118 for decrypting
10 the multicast session data.

Referring again to Figure 1B, last hop router 120 is the last routing entity through which IP data destined for user terminal 110 passes. Last hop router 120 comprises routing function 121, group membership management 122, multicast security unit 123, multicast charging unit 124, data volume meter 125, and charging database 126. Routing function 121 performs
15 traditional network routing and provides support for the IP multicast protocol. Group membership management 122 maintains the group membership information for every terminal on the same multicast link and is responsible for determining the join status of each terminal. Multicast security unit 123 is responsible for sending decryption key 118 to user terminal 110. Optionally, multicast security unit 123 may encrypt the multicast data from multicast server 190
20 before it is sent to user terminal 110. Multicast security unit 123 sends decryption key 118 when the user initially joins a multicast session. Multicast security unit 123 updates decryption key 118 either when another multicast user terminates the session or at discrete time intervals. Multicast security unit 143 communicates decryption key 118 to multicast security client 113

either by a direct connection, via routing function 121, or via routing function 121 and group membership management 122. Multicast charging unit 124 maintains information related to multicast session charges for user terminal 110. Multicast charging unit 124 creates a charging entry in charging database 126 when user terminal 110 joins a multicast session. Multicast charging unit 124 updates the charging entry when user terminal 110 updates the join status or terminates the session. When user terminal 110 terminates the session, multicast charging unit 124 retrieves the relevant session charge information from charging database 126 and forwards the information to billing server 170. Data volume meter 125 measures, for a multicast session, the number of bytes or data volume transmitted to user terminal 110. Charging database 126 stores information related to multicast session charges. The implementation of charging database 126 contemplates a flat-file architecture, relational database management system design, object-oriented database design, or the equivalent.

Referring again to Figure 1B, billing server 170 is a general-purpose server computer that includes a module to convert charging information such as connection time or data volume into billing data including the cost to receive the multicast session data. Billing server 170 comprises billing unit 171 and billing database 172. Billing unit 171 converts the information related to multicast session charges into billing information. Billing database 172 stores the billing information. The implementation of billing database 172 contemplates a flat-file architecture, relational database management system design, object-oriented database design, or the equivalent.

Figure 1C is a network diagram illustrating an embodiment of the secure billing system shown in Figure 1A that accommodates an indirect connection between user terminal 110 and multicast data network 105. Internet 100 and multicast data network 105 perform the same

functions as described above in the discussion of Figure 1A. Bi-directional network 106 is a data network such as a General Packet Radio Service (GPRS) network that supports uplink connectivity and provides an interface between user terminal 110 and multicast data network 105. Uni-directional network 107 is a data network such as a DVB terrestrial (DVB-T) network that transmits multicast data to entities such as user terminal 110. The invention disclosed herein contemplates network architectures comparable to bi-directional network 106 and uni-directional network 107 such as a cellular network, a satellite network, a DVB network, or a private network architecture.

As shown in Figure 1C, user terminal 110 includes an interface module that connects a user to the secure billing system for multicast network services. In one embodiment, user terminal 110 is a mobile device such as a cellular telephone. User terminal 110 also includes a communication module to receive multicast data transmitted by multicast serving node 130. A user operates user terminal 110 to receive multicast content 195 by sending join request 117 to multicast serving node 130 via bi-directional network 106. After receiving join request 117, multicast serving node 130 attaches to the multicast tree using any existing multicast routing protocol. In one embodiment, multicast serving node 130 attaches to the multicast tree via border gateway 180. Multicast serving node 130 and border gateway 180 perform routing functions for multicast data network 105. Multicast serving node 130 forwards the multicast data from multicast data network 105 to user terminal 110 via either bi-directional network 106 or uni-directional network 107. Border gateway 180 is the routing entity that provides the interface between multicast data network 105 and an external network such as Internet 100. In response to join request 117, user terminal 110 receives decryption key 118 from multicast serving node 130 via bi-directional network 106. In one embodiment, multicast serving node

130 is responsible for sending decryption key 118 to user terminal 110 and encrypts the data sent by multicast server 190 prior to forwarding the data to user terminal 110. Multicast serving node 130 also forwards the multicast data comprising multicast content 195 to user terminal 110 via uni-directional network 107. In addition to data routing, multicast serving node 130 monitors
5 multicast communication messages that user terminal 110 sends and receives, stores charging data related to a subscription request, and forwards the charging data to billing server 170, a general-purpose server computer. Billing server 170 converts the charging data into billing data, stores the billing data, and notifies the user of the total charge for subscribing to multicast content 195.

207730-02202
40 An example of the embodiment shown in Figure 1C includes delivering IP data from an Internet Service Provider (ISP) network owned by operator A via a DVB terrestrial (DVB-T) network owned by operator B to the mobile terminal operated by a user. A service agreement between the user and operator A obligates the user to pay a fee for receiving multicast data that operator A delivers. Also, an agreement between operator A and operator B obligates operator A to pay a fee for sending data over the DVB-T network owned by operator B. To subscribe to a
45 multicast session, the user sends join request 117 to multicast serving node 130 via the data network owned by operator C. Multicast serving node 130 delivers multicast session data to the mobile terminal via the DVB-T network owned by operator B, monitors multicast communication messages, stores charging data related to the subscription request, and forwards
20 the charging data to billing server 170.

Figure 1D is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1C. Except for the differences described below, the function and structure of the components shown in Figure 1D are identical to the components shown in Figure

1B. Multicast serving node 130 performs the functions described for last hop router 120 in the discussion of Figure 1B. In Figure 1D, routing function 131 and multicast security unit 133 do not communicate with user terminal 110 directly, but via either bi-directional network 106 or uni-directional network 107. Similarly, multicast session management 112 does not
5 communicate with multicast serving node 130 directly, but via bi-directional network 106.

Figure 1E is a network diagram illustrating an embodiment of the secure billing system shown in Figure 1A that distributes the security function to base station 140 and the charging function to charging server 150. As shown in Figure 1E, user terminal 110 is a mobile device that communicates with wireless network 108 via base station 140. In one embodiment, base station 140 is the base station subsystem in a GPRS network. A user operates user terminal 110 to receive multicast content 195 by sending join request 117 to base station 140. After receiving join request 117, base station 140 attaches to the multicast tree using any existing multicast routing protocol. In one embodiment, base station 140 attaches to the multicast tree via last hop router 120 and border gateway 180. Last hop router 120 and border gateway 180 perform
10 routing functions for wireless network 108. In response to join request 117, user terminal 110 receives decryption key 118 from base station 140. In one embodiment, base station 140 is responsible for sending decryption key 118 to user terminal 110 and encrypts the data sent by multicast server 190 prior to forwarding the data to user terminal 110. In addition to data routing, the connection between last hop router 120 and base station 140 allow last hop router
15 120 to monitor multicast communication messages that user terminal 110 sends to and receives from base station 140. Last hop router 120 also transfers charging data related to a subscription request to charging server 150. In one embodiment, charging server 150 stores the charging data and periodically forwards the data via a direct connection to billing server 170. In another

embodiment, charging server 150 stores the charging data and periodically forwards the data to billing server 170 via a connection between last hop router 120 and billing server 170. Charging server 150 and billing server 170 are general-purpose server computers.

Figure 1F is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1E. Except for the differences described below, the function and structure of the components shown in Figure 1F are identical to the components shown in Figure 1B. Figure 1F distributes the components of last hop router 120, as shown in Figure 1B, among last hop router 120, base station 140, and charging server 150. Last hop router 120 comprises routing function 121, group membership management 122, and data volume meter 125. Base station 140 comprises multicast security unit 123, the communication interface between multicast security unit 123 and routing function 121, and the communication interface between multicast security unit 123 and group membership management 122. Charging server 150 comprises multicast charging unit 124, charging database 126, the communication interface between multicast charging unit 124 and group membership management 122, and the communication interface between multicast charging unit 124 and data volume meter 125. In one embodiment, billing server 170 comprises billing unit 171 and billing database 172 and charging server 150 further comprises a communication interface between charging unit 124 and billing unit 171.

Figure 1G is a network diagram that illustrates the components comprising the secure billing system shown in Figure 1E. Except for the differences described below, the function and structure of the components shown in Figure 1G are identical to the components shown in Figure 1F. Figure 1G illustrates a distributed architecture for group membership management 122 shown in Figure 1F. Last hop router 120, as shown in Figure 1G, comprises routing function

121, data volume meter 125, and network layer group membership management 128. Base station 140, as shown in Figure 1G, comprises multicast security unit 123, link layer group membership management 127, the communication interface between multicast security unit 123 and routing function 121, and the communication interface between link layer group membership management 127 and network layer group membership management 128. Charging server 150, as shown in Figure 1G, comprises multicast charging unit 124, charging database 126, the communication interface between multicast charging unit 124 and network layer group membership management 128, and the communication interface between multicast charging unit 124 and data volume meter 125. Link layer group membership management 127 maintains the information of the join status of user terminal 110 within the cell and provides that information to multicast charging unit 124. Whenever there are any multicast receivers within the cell, link layer group membership management 127 informs network layer group membership management 128 to join the multicast tree. Network layer group membership management 128 is responsible for keeping track of which base station needs multicast data and routes the multicast data to the appropriate base station.

Figures 2A and 2B illustrate a method of operation for the secure billing system shown in Figure 1B. Referring to Figures 1A and 2A, the method begins at step 202 with multicast server 190 announcing the available multicast sessions to user terminal 110 via multicast data network 105. At step 204, service discovery 111 discovers the multicast sessions that are available. Service discovery 111 provides an operator of user terminal 110 with a list of available multicast sessions and the relevant information for each session. The relevant information includes the starting time and cost associated with a multicast session. The operator selects a multicast session from the list. In response to the operator's selection, user terminal 110 activates the

selected multicast session. In one embodiment, the activation of the multicast session occurs immediately. In another embodiment, the activation occurs at a predetermined time such as before the start of the multicast session. At step 206, multicast session management 112 sends join request 117 for the selected multicast session to group membership management 122.

5 Group membership management 122 receives join request 117 at step 208 and records the join status of the user terminal at step 212. Group membership management 122 forwards the joined status information to multicast charging unit 124 and multicast security unit 123. Multicast charging unit 124 uses the joined status information to create a charging entry in charging database 146 at step 214. Multicast security unit 123 uses the joined status information to send a decryption key to user terminal 110 at step 216 which multicast security client 113 receives at step 218 before receiving multicast session data at step 220. In one embodiment, multicast security unit 123 encrypts the message prior to sending the decryption key and multicast security client 113 decrypts the message after receiving the decryption key. After receiving join request 117 at step 208, group membership management 122 also attaches to the multicast tree using any multicast routing protocol at step 210. In one embodiment, group membership management 122 applies authentication and authorization procedures before attaching to the multicast tree. At step 222, multicast server 190 sends multicast session data to multicast security unit 123. The multicast session data is encrypted by multicast security unit 123 at step 224 and decrypted by multicast security client 113 at step 226 before receiving multicast session data at step 220.

20 At step 228, Figure 2A illustrates user terminal 110 updating the join status, for example, to extend the duration of the multicast session connection. Multicast session management 112 resends the join request to group membership management 122. Group membership management 122 updates the join status for user terminal 110 at step 230 and notifies multicast

security unit 123 to send an updated decryption key at step 216. Multicast session management 112 is responsible for sending an updated join request to last hop router 120 on an on-going basis. As long as the user is receiving the session, multicast session management 113 must update the join status for the terminal before it expires. Whenever the join status is updated, group membership management 122 also forwards the status to multicast charging unit 124 to update the charging entry at step 232. After updating the join status for user terminal 110 at step 230, group membership management 122 notifies multicast charging unit 124 to update the charging entry in charging database 126 at step 232.

At step 234, Figure 2B illustrates user terminal 110 terminating the multicast session, either explicitly or implicitly, by sending a disjoin message to last hop router 140. Group membership management 122 receives the disjoin message and, at step 236, notifies multicast charging unit 124 to close the charging entry for user terminal 110 in charging database 126. Multicast charging unit 124 forwards the charging data to billing server 170 at step 238. Billing server 170 converts the charging data to billing data, at step 240, and sends the billing data to the user at step 242. If a data volume based charging mechanism is used, in order to generate and update the charging entry, data volume meter 125 forwards to multicast charging unit 124 the volume of data delivered to user terminal 110. At step 244, group membership management 122 determines whether any receivers of the multicast data have an active join status. If no receivers have an active join status, at step 246, group membership management 122 detaches user terminal 110 from the multicast tree. If there is at least one receiver with an active status, group membership management 122 proceeds to steps 230 and 216 where the terminal status is updated and multicast security unit 123 is notified to send an updated decryption key to multicast security client 113.

Figures 2C and 2D illustrate a method of operation for the secure billing system shown in Figure 1G. Referring to Figures 1E and 2C, the method begins at step 202 with multicast server 190 announcing the available multicast sessions to user terminal 110 via wireless network 108. At step 204, service discovery 111 discovers the multicast sessions that are available. Service discovery 111 provides an operator of user terminal 110 with a list of available multicast sessions and the relevant information for each session. The relevant information includes the starting time and cost associated with a multicast session. The operator selects a multicast session from the list. In response to the operator's selection, user terminal 110 activates the selected multicast session. In one embodiment, the activation of the multicast session occurs immediately. In another embodiment, the activation occurs at a predetermined time such as before the start of the multicast session. At step 206, multicast session management 112 sends join request 117 for the selected multicast session to link layer group membership management 127. Link layer group membership management 127 receives join request 117 at step 208 and records the join status of the user terminal at step 212. Link layer group membership management 127 forwards the joined status information to multicast charging unit 124 and multicast security unit 123. Multicast charging unit 124 uses the joined status information to create a charging entry in charging database 146 at step 214. Multicast security unit 123 uses the joined status information to send a decryption key to user terminal 110 at step 216 which multicast security client 113 receives at step 218 before receiving multicast session data at step 220. In one embodiment, multicast security unit 123 encrypts the message prior to sending the decryption key and multicast security client 113 decrypts the message after receiving the decryption key. After receiving join request 117 at step 208, link layer group membership management 127 also notifies network layer group membership management 128 to attach to the

multicast tree using any multicast routing protocol at step 210. In one embodiment, link layer group membership management 127 applies authentication and authorization procedures before attaching to the multicast tree. At step 222, multicast server 190 sends multicast session data to multicast security unit 123. The multicast session data is encrypted by multicast security unit 123 at step 224 and decrypted by multicast security client 113 at step 226 before receiving multicast session data at step 220.

At step 228, Figure 2C illustrates user terminal 110 updating the join status, for example, to extend the duration of the multicast session connection. Multicast session management 112 resends the join request to link layer group membership management 127. Link layer group membership management 127 updates the join status for user terminal 110 at step 230 and notifies multicast security unit 123 to send an updated decryption key at step 216. Multicast session management 112 is responsible for sending an updated join request to last hop router 120 on an on-going basis. As long as the user is receiving the session, multicast session management 113 must update the join status for the terminal before it expires. Whenever the join status is updated, link layer group membership management 127 also forwards the status to multicast charging unit 124 to update the charging entry at step 232. After updating the join status for user terminal 110 at step 230, link layer group membership management 127 notifies multicast charging unit 124 to update the charging entry in charging database 126 at step 232.

At step 234, Figure 2D illustrates user terminal 110 terminating the multicast session, either explicitly or implicitly, by sending a disjoin message to last hop router 140. Link layer group membership management 127 receives the disjoin message and, at step 236, notifies multicast charging unit 124 to close the charging entry for user terminal 110 in charging database 126. Multicast charging unit 124 forwards the charging data to billing server 170 at step 238.

Billing server 170 converts the charging data to billing data, at step 240, and sends the billing data to the user at step 242. If a data volume based charging mechanism is used, in order to generate and update the charging entry, data volume meter 125 forwards to multicast charging unit 124 the volume of data delivered to user terminal 110. At step 244, link layer group membership management 127 determines whether any receivers of the multicast data have an active join status. If no receivers have an active join status, link layer group membership management 127 notifies network layer group membership management 128, at step 246, to detach user terminal 110 from the multicast tree. If there is at least one receiver with an active status, link layer group membership management 127 proceeds to steps 230 and 216 where the terminal status is updated and multicast security unit 123 is notified to send an updated decryption key to multicast security client 113.

Connection Time Charging

A charging scheme based on connection time calculates a fee for a service from the elapsed time that a user connects to the service. For example, if a network operator determines that the rate for using a video service is \$5.00 per hour, a user connecting to the video service to view a movie for thirty-minutes accrues a fee of \$2.50. In a multicast network, a charging scheme based on connection time is most beneficial when an average multicast session has a fixed bandwidth. Determination of the connection time involves storing the time that the user terminates the multicast session connection, storing the time that the user initiates the multicast session connection, and calculating the difference between these times. Since a multicast session is dynamic, the challenge is to determine when the initiation and termination of the connection occurs.

The packets that comprise a multicast session are encrypted. Thus, a user cannot receive the multicast session without explicitly requesting to join a multicast group and receiving a decryption key. Referring to Figure 1B, service discovery 171 receives all the available multicast sessions from last hop router 140. When user terminal 170 selects and activates a multicast session, multicast session management 172 explicitly requests to join a multicast group by sending join message 160 to group membership management 142. In response, group membership management 142 notifies multicast charging unit 144 and multicast security unit 143 that user terminal 170 agrees to pay a fee based on the connection time to the multicast service. Multicast charging unit 144 creates a charging entry for user terminal 170 and multicast content 110. Multicast security client 173 receives decryption key 165 from multicast security unit 143 that will decrypt the multicast session packet data. Group membership management 142 receives every join message sent by a user of the multicast service associated with a multicast group. A validated or authenticated join message activates the “joined” status for the user who sent the join message. Multicast charging unit 144 creates and maintains an entry in charging database 146 for each validated join message. The entry in charging database 146 comprises user identification data, session identification data, a cumulative connection time, and an expiration time for the “joined” status.

The join message sent by the user identifies the requested multicast session, the requested start time for the charging, and the requested stop time for the charging. The join message obligates the user to pay the charges that accrue from the start time to the end time. When the user has “joined” status, the multicast network is responsible for updating the user’s “decryption key” whenever host membership in the multicast group changes. For a discussion of several

methods for delivery of the decryption key see "Secure Group Communication using Key Graphs", IEEE/ACM Transactions on Networking, February 2000.

The stop time specified in the join message is the initial stop time for the user's multicast session. The user can extend the stop time by sending a second join message to specify a later stop time. The stop time can only be extended if group membership management 142 receives the second join message prior to the initial stop time. If the second join message arrives after the first join status expires, the user will be disconnecting with the multicast session first as a result of the expired join status. When the second join message arrives, it will act as a new join message to connect user terminal 110 to the multicast session. Following the receipt of a second or subsequent join message, multicast charging unit 144 updates the entry for the user and multicast session in charging database 146 and notifies other group members of a membership change.

In one embodiment, the interval between the start time and the stop time in each join message can be determined based on the configuration set by either the user or network operator. In another embodiment, the interval between the start time and the stop time can be calculated according to an environmental characteristic including the velocity of the terminal, the strength of the reception signal, and the quality of the reception signal.

Termination of the multicast session can happen either explicitly or implicitly. Explicit termination of the multicast session occurs when the user sends a disjoin message that specifies a stop time earlier than the pending stop time. A disjoin message is only effective, however, if group membership management 142 receives the disjoin message prior to the pending stop time. Following receipt of a disjoin message, multicast charging unit 144 updates and closes the entry in charging database 146 and forwards the charging data to billing unit 151 for conversion into

billing data and storage in billing database 152. If the forwarding of the charging data is successful, multicast charging unit 144 deletes the entry in charging database 146 and, if the second join message arrives after the first join status expires, multicast security unit 143 updates decryption key 165 for other group members of the same multicast session. Implicit termination of the multicast session occurs when the user's "joined" status expires before the user sends a subsequent join message to extend the stop time. An implicit termination may occur, for example, when the battery in the user's terminal loses power or some other reason that causes terminal to loose the network connection. Accounting for implicit termination of a multicast session ensures that an excessive charge does not accrue for the user.

When the user status changes state from "joined" to "disjoined", multicast charging unit 144 calculates the total connection time. The billing related information such as user identification data, session identification data, and connection time is transferred from multicast charging unit 144 to billing server 150. Then, billing unity 151 converts the charging data into billing data and stores the billing data in billing database 152. Alternatively, multicast charging unit 144 periodically transfers billing data to billing server 150.

UNRESTRICTED CONNECTION TIME

Figures 3A and 3B are exemplary timelines for a charging scheme based on connection time that allows a user to join or leave a multicast session at any time. Referring to Figures 1B and 3A, if user terminal 170 explicitly requests termination of the multicast session connection, determination of the connection time comprises:

1. User terminal 170 sending a join message to group membership management 142 at time t_{X0} .

If the join message takes the form $\text{join}(p, t_{S1}, t_{E1})$, the user is requesting to join multicast session p , start the connection time charging at time t_{S1} , and end the connection time charging

at time t_{E1} . If the user wants to start the connection time charging immediately, t_{S1} is set equal to null.

2. Multicast security client 173 receiving decryption key 165 from multicast security unit 143 before time t_{S1} . Decryption key 165 functions to decrypt the packet data comprising multicast session p .
3. At time t_{S1} , multicast charging unit 144 adds an entry to charging database 146 to track connection time charges for user terminal 170 using multicast session p . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_{E1} - t_{S1})$	t_{E1}

If the user sets t_{S1} in the join message equal to null to indicate that the connection time charging will start immediately, t_{X0} will replace t_{S1} in the charging table because the join message was sent at time t_{X0} .

4. From time t_{S1} until time t_{E1} , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes.
5. At time t_{X1} , where $t_{X1} < t_{E1}$, user terminal 170 extends the stop time by sending a second join message to specify a later stop time. If the second join message takes the form $\text{join}(p, t_{E1}, t_{E2})$, the user is requesting to extend the end time for the connection to multicast session p from time t_{E1} to time t_{E2} .
6. At time t_{E1} , multicast charging unit 144 updates the entry in charging database 146 to track connection time charges for user terminal 170 using multicast session p . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_{E1} - t_{S1})$ $+ (t_{E2} - t_{E1})$	t_{E2}

7. From time t_{E1} until time t_{E2} , the multicast network is responsible for updating the "decryption key" for user terminal 170 whenever host membership in the multicast group changes.
8. At time t_{X2} , where $t_{X2} < t_{E2}$, user terminal 170 sends a disjoin message that specifies a stop time earlier than the pending stop time, t_{E2} . If the disjoin message takes the form $\text{leave}(p, t_{E3})$, user terminal 170 is requesting to leave multicast session p at time t_{E3} . If user terminal 170 wants to leave multicast session p immediately, t_{E3} is set equal to null. Multicast charging unit 144 updates the entry in charging database 146 to track connection time charges for user terminal 170 using multicast session p . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_{E1} - t_{S1})$ $+ (t_{E2} - t_{E1})$ $+ (t_{E3} - t_{E2})$	t_{E3}

- If the user sets t_{E3} in the disjoin message equal to null to indicate that user terminal 170 wants to leave multicast session p immediately, t_{X2} will replace t_{E3} in the charging table because the join message was sent at time t_{X2} .
9. At time t_{E3} , collection of connection time charges for user terminal 170 stops. The multicast network is responsible for updating the "decryption key" for the other group members because user terminal 170 disjoined the multicast group. Since the collection of connection time charges has stopped, multicast charging unit 144 closes the entry in charging database 146 for user terminal 170 using multicast session p , communicates the charging data to

billing unit **151** for storage in billing database **152**, and deletes the entry in charging database **146**.

Referring to Figures **1B** and **3B**, if termination of the multicast session connection is implied from the passage of time, steps 1 through 7 are identical to steps 1 through 7 from the discussion of Figure **3A** and determination of the connection time comprises:

1. User terminal **170** sending a join message to group membership management **142** at time t_{X0} .
If the join message takes the form $\text{join}(p, t_{S1}, t_{E1})$, the user is requesting to join multicast session p , start the connection time charging at time t_{S1} , and end the connection time charging at time t_{E1} . If the user wants to start the connection time charging immediately, t_{S1} is set equal to null.
2. Multicast security client **173** receiving decryption key **165** from multicast security unit **143** before time t_{S1} . Decryption key **165** functions to decrypt the packet data comprising multicast session p .
3. At time t_{S1} , multicast charging unit **144** adds an entry to charging database **146** to track connection time charges for user terminal **170** using multicast session p . In one embodiment, the entry to charging database **146** appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_{E1} - t_{S1})$	t_{E1}

If the user sets t_{S1} in the join message equal to null to indicate that the connection time charging will start immediately, t_{X0} will replace t_{S1} in the charging table because the join message was sent at time t_{X0} .

4. From time t_{S1} until time t_{E1} , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes.
5. At time t_{X1} , where $t_{X1} < t_{E1}$, user terminal 170 extends the stop time by sending a second join message to specify a later stop time. If the second join message takes the form $\text{join}(p, t_{E1}, t_{E2})$, the user is requesting to extend the end time for the connection to multicast session p from time t_{E1} to time t_{E2} .
6. At time t_{E1} , multicast charging unit 144 updates the entry in charging database 146 to track connection time charges for user terminal 170 using multicast session p . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_{E1} - t_{S1})$ $+ (t_{E2} - t_{E1})$	t_{E2}

7. From time t_{E1} until time t_{E2} , the multicast network is responsible for updating the "decryption key" for user terminal 170 whenever host membership in the multicast group changes.
8. At time t_{E2} , the connection time charging for user terminal 170 expires. Multicast charging unit 144 stops updating the entry for user terminal 170 using multicast session p in charging database 146. Multicast charging unit 144 communicates with billing server 150 to transfer the charging data for user terminal 170 using multicast session p from charging database 146 to billing database 151. Billing unit 151 converts the connection time, data volume, or other form of information for user terminal 170 using multicast session p to the entry of billing database 151, which has information of total cost of multicast session for user terminal 170. Alternatively, the entry in charging database 146 is transferred periodically to billing server 150. In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_{E1} - t_{S1})$ $+ (t_{E2} - t_{E1})$	t_{E2}

HANDOVER

The following examples describe how the system performs charging when a handover occurs from node A to node B. In the first example, the system configuration is as shown in Figure 1B and the handover is from one last hop router to another. User terminal 110 needs to send a new join message to node B and a disjoin message to node A. Alternatively, node B can inform node A of the handover and disjoin user terminal 110 from node A. All of the components in node A (group membership management 122, multicast charging unit 124, multicast security unit 124, etc.) will follow the disjoin procedure as described herein. All of the components in node B (group membership management 122, multicast charging unit 124, multicast security unit 124, etc.) will follow the join procedure as described herein.

In the second example, the system configuration is as shown in Figure 1B and nodes A and B are equipped with independent group membership management components or link layer group membership management components, but share the same multicast charging unit or charging server. User terminal 110 joins the multicast session from node A and later performs a handover from node A to node B. Since node A and node B are both equipped with group membership management or link layer group membership management components, the nodes support charging in a handover situation if a column is added to the charging entry to identify which node is responsible for the charging entry. When node A, in response to a join request, instructs multicast charging unit 124 to create a charging entry for user terminal 110, the ID of node A (e.g., the IP address of node A) is recorded in the charging entry as the "node responsible

for this charging entry". When user terminal 110 performs a handover from node A to node B, user terminal 110 sends a join request to node B. As a result, node B sends a request for creating charging entry to multicast charging unit 124 that is shared by node A and node B. Upon receiving such a request, multicast charging unit 124 updates the relevant entry by changing the "node responsible for this charging entry" to node B and updating the "joined status expire time" to the new one indicated in the new join message. In addition, multicast charging unit 124 informs node A that node A is no longer responsible for the charging entry associated with user terminal 110. Node a may perform the disjoin procedure described herein to disjoin user terminal 110 from node A.

For example, before handover, user terminal 110 receives multicast data via node A. The charging entry is:

User Identification	Session Identification	Node Responsible for this Entry	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	ID of node A	$(t_{E1} - t_{S1})$ $+ (t_{E2} - t_{E1})$ $+ (t_{E3} - t_{E2})$	t_{E3}

Then user terminal 110 begins to perform the handover. At time t_{H1} , where $t_{X2} < t_{E3}$, node B with group membership management component receives the join message $\text{join}(p, \text{null}, t_{E4})$ from user terminal 110. Node B informs multicast charging unit 124 to create a charging entry for user terminal 110. In response, multicast charging unit 124 modifies the existing charging entry in the following manner.

User Identification	Session Identification	Node Responsible for this Entry	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	ID of node B	$(t_{E1} - t_{S1})$ $+ (t_{E2} - t_{E1})$ $+ (t_{E4} - t_{E2})$	t_{E4}

Also, multicast charging unit **124** will inform node A that node A is no longer responsible for the charging entry associated with user terminal **110**. Node A may perform disjoin procedures to disjoin user terminal **110** from node A.

SLOTTED CONNECTION TIME

5 Figures **3C** and **3D** are exemplary timelines for a charging scheme based on connection time that only allows a user to join or leave a multicast session at the end of a discrete point in time or time slot. Since the user can only join or leave the multicast session at slotted time intervals (i.e., discrete points in time), the network only needs to update to the decryption key at those discrete points in time. Thus, the network can synchronize the disjoin activity of multiple users and reduce the number of decryption keys delivered. Referring to Figures **1B** and **3C**, if user terminal **170** explicitly requests termination of the multicast session connection, determination of the connection time comprises:

1. User terminal **170** sending a join message to group membership management **142** at time t_{X0} .
If the join message takes the form $\text{join}(p, t_{S1}, 2)$, the user is requesting to join multicast session p , start the connection time charging at time t_{S1} , and pay for the service from the start time until time $t_3 = [(t_0 + m - t_{S1}) + (2 \times m)]$ where m is the duration of a time slot and t_0 is the start of a time slot.
2. Multicast security client **173** receiving decryption key **165** from multicast security unit **143** before time t_{S1} . The multicast network informs user terminal **170** that time t_{D1} is the deadline for extending the expiration of the connection to multicast session p . The offset w is defined by the network and represents the time interval between the deadline for receiving another join message and the end of a time slot.

3. At time t_{S1} , multicast charging unit 144 adds an entry to charging database 146 to track connection time charges for user terminal 170 using multicast session p . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$[(t_0 + m - t_{S1}) + (2 \times m)]$	t_3

4. From time t_{S1} until time t_3 , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes. The updates to decryption key 165 occur during the offset interval w for each time slot. During the offset interval w , if the network determines that the status for a user will change from "joined" to "disjoined", the network updates decryption key 165.

5. At time t_{X1} , where $t_{X1} < t_{D1}$, user terminal 170 extends the stop time by sending a second join message to specify a later stop time. If the second join message takes the form $\text{join}(p, t_3, 2)$, the user is requesting to extend the end time for the connection to multicast session p for 2 time slots after time t_3 . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$[(t_0 + m - t_{S1}) + (2 \times m) + (2 \times m)]$	t_5

The multicast network informs user terminal 170 that time t_{D2} is the deadline for extending the expiration of the connection to multicast session p .

6. From time t_3 to time t_5 , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes.

7. At time t_{X2} , where $t_{X2} < t_{D2}$, user terminal 170 sends a disjoin message that specifies to stop accruing a fee when the current time slot expires. If the disjoin message takes the form $\text{leave}(p, 0)$, user terminal 170 is requesting to leave session p when the current time slot expires. In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_0 + m - t_{S1})$ $+ (2 \times m) + (2 \times m)$ $- (t_5 - t_4)$	t_4

8. After time $(t_4 - w)$, if the network determines that the status for a user will change from "joined" to "disjoined", the network updates decryption key 165 and continues the multicast session for the user into the next time slot.
9. At time t_4 , collection of connection time charges for user terminal 170 stops. The multicast network is responsible for updating the "decryption key" for the other group members because user terminal 170 disjoined the multicast group. Since the collection of connection time charges has stopped, multicast charging unit 144 closes the entry in charging database 146 for user terminal 170 using multicast session p , communicates the charging data to billing unit 151 for storage in billing database 152, and deletes the entry in charging database 146.

Referring to Figures 1B and 3D, if termination of the multicast session connection is implied from the passage of time, steps 1 through 6 are identical to steps 1 through 6 from the discussion of Figure 3C and determination of the connection time comprises:

1. User terminal 170 sending a join message to group membership management 142 at time t_{X0} . If the join message takes the form $\text{join}(p, t_{S1}, 2)$, the user is requesting to join multicast session p , start the connection time charging at time t_{S1} , and pay for the service from the start

time until time $t_3 = [(t_0 + m - t_{S1}) + (2 \times m)]$ where m is the duration of a time slot and t_0 is the start of a time slot.

2. Multicast security client **173** receiving decryption key **165** from multicast security unit **143** before time t_{S1} . The multicast network informs user terminal **170** that time t_{D1} is the deadline for extending the expiration of the connection to multicast session p . The offset w is defined by the network and represents the time interval between the deadline for receiving another join message and the end of a time slot.
3. At time t_{S1} , multicast charging unit **144** adds an entry to charging database **146** to track connection time charges for user terminal **170** using multicast session p . In one embodiment, the entry to charging database **146** appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$[(t_0 + m - t_{S1}) + (2 \times m)]$	t_3

4. From time t_{S1} until time t_3 , the multicast network is responsible for updating decryption key **165** for user terminal **170** whenever host membership in the multicast group changes. The updates to decryption key **165** occur during the offset interval w for each time slot. During the offset interval w , if the network determines that the status for a user will change from "joined" to "disjoined", the network updates decryption key **165**.
5. At time t_{X1} , where $t_{X1} < t_{D1}$, user terminal **170** extends the stop time by sending a second join message to specify a later stop time. If the second join message takes the form $\text{join}(p, t_3, 2)$, the user is requesting to extend the end time for the connection to multicast session p for 2 time slots after time t_3 . In one embodiment, the entry to charging database **146** appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$[(t_0 + m - t_{S1}) + (2 \times m) + (2 \times m)]$	t_5

The multicast network informs user terminal 170 that time t_{D2} is the deadline for extending the expiration of the connection to multicast session p .

6. From time t_3 to time t_5 , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes.

5 7. After time t_{D2} , if the network determines that the status for a user will change from "joined" to "disjoined", the network updates decryption key 165 and continues the multicast session for the user into the next time slot.

8. At time t_5 , collection of connection time charges for user terminal 170 stops. The multicast network is responsible for updating the "decryption key" for the other group members because user terminal 170 disjoined the multicast group. Since the collection of connection time charges has stopped, multicast charging unit 144 closes the entry in charging database 146 for user terminal 170 using multicast session p , communicates the charging data to billing unit 151 for storage in billing database 152, and deletes the entry in charging database 146. Alternatively, multicast charging unit 144 transfers the entry directly to billing server

15 150. In another embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Connection Time	Expiration Time of "Joined" Status
21323421	finnkino 457286529 1453 172.10.20.212	$(t_0 + m - t_{S1}) + (2 \times m) + (2 \times m)$	t_5

Data Volume Based Charging

A charging scheme based on the volume of data calculates a fee for a service from the volume of data that a user receives from the service. For example, if a network operator determines that the rate for using a video service is \$0.25 for each Megabyte of data received, a user connecting to the video service to view a movie consisting of 25 Megabytes of data accrues a fee of \$6.25. In a multicast network, a charging scheme based on the volume of data is most beneficial when the data rate varies. Similar to the charging scheme based on connection time discussed above, the connectivity and security is managed on time basis, however, determination of charge requires accounting for the number of bytes transferred during the connection time.

Figures 4A and 4B are exemplary timelines for a charging scheme based on data volume that only allows a user to join or leave a multicast session at the end of a discrete point in time or time slot. Referring to Figures 1B and 4A, if user terminal 170 explicitly requests termination of the multicast session connection, determination of the data volume comprises:

1. Data volume meter 145 examining IP multicast data packets and maintaining a tally of the number of bytes of data received, for a given destination address and multicast session. Data volume meter 145 can either be co-located with multicast charging unit 144 or located on an upper layer of the multicast tree (e.g., on the gateway router where the multicast data enters the multicast network). In one embodiment, each last hop router may include a meter for measuring the multicast session routed to the last hop router. In another embodiment, the meter can be distributed across several access routers in the multicast network.
2. User terminal 170 sending a join message to group membership management 142 at time t_{X0} . If the join message takes the form $\text{join}(p, t_{S1}, 2)$, the user is requesting to join multicast session p , start the connection time charging at time t_{S1} , and pay for the service from the start

time until time $t_3 = [(t_0 + m - t_{S1}) + (2 \times m)]$ where m is the duration of a time slot and t_0 is the start of a time slot. Calculation of the fee depends on the volume of data received by a given destination and multicast session between time t_{S1} and t_3 .

3. Multicast security client **173** receiving decryption key **165** from multicast security unit **143** before time t_{S1} . The multicast network informs user terminal **170** that time t_{D1} is the deadline for sending another join message. The offset w is defined by the network and represents the time interval between the deadline for receiving another join message and the end of a time slot.
4. At time t_{S1} , data volume meter **145** signals multicast charging unit **144** to add an entry to charging database **146** to store the data volume start value, V_1 , for user terminal **170** using multicast session p . In one embodiment, the entry to charging database **146** appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of "Joined" Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	Null	t_3

5. From time t_{S1} until time t_3 , the multicast network is responsible for updating decryption key **165** for user terminal **170** whenever host membership in the multicast group changes. The updates to decryption key **165** occur during the offset interval w for each time slot. During the offset interval w , if the network determines that the status for a user will change from "joined" to "disjoined", the network updates decryption key **165**.
6. At time t_{X1} , where $t_{X1} < t_{D1}$, user terminal **170** extends the stop time by sending a second join message to specify a later stop time. If the second join message takes the form $\text{join}(p, t_3, 2)$,

the user is requesting to extend the end time for the connection to multicast session p for 2 time slots after time t_3 . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of "Joined" Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	Null	t_5

The multicast network informs user terminal 170 that time t_{D2} is the deadline for extending the expiration of the connection to multicast session p .

7. From time t_3 to time t_5 , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes.
8. At time t_{X2} , where $t_{X2} < t_{D2}$, user terminal 170 sends a disjoin message that specifies to stop accruing a fee when the current time slot expires. If the disjoin message takes the form $\text{leave}(p, 0)$, user terminal 170 is requesting to leave session p when the current time slot expires. In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of "Joined" Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	Null	t_4

9. After time $(t_4 - w)$, if the network determines that the status for a user will change from "joined" to "disjoined", the network updates decryption key 165 and continues the multicast session for the user into the next time slot.

10. At time t_4 , collection of the data volume charges for user terminal 170 stops. Data volume meter 145 communicates the data volume end value, V_2 , for user terminal 170 using multicast session p to multicast charging unit 144. Multicast charging unit 144 updates the entry to charging database 146. In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of "Joined" Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	V_2	t_4

Since the collection of data volume charges has stopped, multicast charging unit 144 closes the entry in charging database 146 for user terminal 170 using multicast session p , communicates the charging data to billing unit 151 for storage in billing database 152, and deletes the entry in charging database 146. Since the charging data is summarized, the total volume of data for user terminal 170 using multicast session p is $(V_2 - V_1)$. In another embodiment, data volume meter 145 communicates the charging data to billing server 150 directly, without storing the charging data in charging database 146.

Referring to Figures 1B and 4B, if termination of the multicast session connection is implied from the passage of time, steps 1 through 7 are identical to steps 1 through 7 from the discussion of Figure 4A and determination of the data volume comprises:

1. Data volume meter 145 examining IP multicast data packets and maintaining a tally of the number of bytes of data received, for a given destination address and multicast session. Data volume meter 145 can either be co-located with multicast charging unit 144 or located on an upper layer of the multicast tree (e.g., on the gateway router where the multicast data enters

the multicast network). In one embodiment, each last hop router may include a meter for measuring the multicast session routed to the last hop router. In another embodiment, the meter can be distributed across several access routers in the multicast network.

2. User terminal 170 sending a join message to group membership management 142 at time t_{X0} .

If the join message takes the form $\text{join}(p, t_{S1}, 2)$, the user is requesting to join multicast session p , start the connection time charging at time t_{S1} , and pay for the service from the start time until time $t_3 = [(t_0 + m - t_{S1}) + (2 \times m)]$ where m is the duration of a time slot and t_0 is the start of a time slot. Calculation of the fee depends on the volume of data received by a given destination and multicast session between time t_{S1} and t_3 .

3. Multicast security client 173 receiving decryption key 165 from multicast security unit 143 before time t_{S1} . The multicast network informs user terminal 170 that time t_{D1} is the deadline for sending another join message. The offset w is defined by the network and represents the time interval between the deadline for receiving another join message and the end of a time slot.

4. At time t_{S1} , data volume meter 145 signals multicast charging unit 144 to add an entry to charging database 146 to store the data volume start value, V_1 , for user terminal 170 using multicast session p . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of "Joined" Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	Null	t_3

5. From time t_{S1} until time t_3 , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes. The updates to decryption key 165 occur during the offset interval w for each time slot. During the offset interval w , if the network determines that the status for a user will change from “joined” to “disjoined”, the network updates decryption key 165.
6. At time t_{X1} , where $t_{X1} < t_{D1}$, user terminal 170 extends the stop time by sending a second join message to specify a later stop time. If the second join message takes the form $\text{join}(p, t_3, 2)$, the user is requesting to extend the end time for the connection to multicast session p for 2 time slots after time t_3 . In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of “Joined” Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	Null	t_5

The multicast network informs user terminal 170 that time t_{D2} is the deadline for extending the expiration of the connection to multicast session p .

7. From time t_3 to time t_5 , the multicast network is responsible for updating decryption key 165 for user terminal 170 whenever host membership in the multicast group changes.
8. After time t_{D2} , if the network determines that the status for a user will change from “joined” to “disjoined”, the network updates decryption key 165 and continues the multicast session for the user into the next time slot.
9. At time t_5 , collection of the data volume charges for user terminal 170 stops. Data volume meter 145 communicates the data volume end value, V_3 , for user terminal 170 using multicast

session p to multicast charging unit 144. Multicast charging unit 144 updates the entry to charging database 146. In one embodiment, the entry to charging database 146 appears as follows:

User Identification	Session Identification	Data Volume on Meter		Expiration Time of "Joined" Status
		Start Value	End Value	
21323421	finnkino 457286529 1453 172.10.20.212	V_1	V_3	t_4

Since the collection of data volume charges has stopped, multicast charging unit 144 closes the entry in charging database 146 for user terminal 170 using multicast session p , communicates the charging data to billing unit 151 for storage in billing database 152, and deletes the entry in charging database 146. Since the charging data is summarized, the total volume of data for user terminal 170 using multicast session p is $(V_3 - V_1)$. In another embodiment, data volume meter 145 communicates the charging data to billing server 150 directly, without storing the charging data in charging database 146.

Although the embodiments disclosed herein describe a fully functioning system, method, and computer program product for calculating a cost of receiving multicast data from a multicast session, the reader should understand that other equivalent embodiments exist. Since numerous modifications and variations will occur to those who review this disclosure, the system, method, and computer program product for calculating a cost of receiving multicast data from a multicast session is not limited to the exact construction and operation illustrated and disclosed herein. Accordingly, this disclosure intends all suitable modifications and equivalents to fall within the scope of the claims.